Insper

Ativos Digitais e Blockchain

Ricardo Rocha
Raul Ikeda

Objetivo

- Introdução à tecnologia Blockchain

Blockchain

- O que é Blockchain?
  - Em poucas palavras: um banco de dados NoSQL descentralizado.

- Vantagens:
  - Auditável
  - Imutável
  - Robusto
  - "Democrático"

- Desvantagens:
  - Baixa performance
  - "Hackeável" (e de várias formas)

- Video Explicativo: https://youtu.be/SSo_EIwHSd4

Blockchain – Quando usar

Pense na sua solução e nas partes envolvidos, respondendo as seguintes perguntas:

- Os recursos e/ou dados são compartilhados entre as partes?
- Sua solução precisa de um intermediário para auditoria?
- Há problemas de confiança entre as partes envolvidas?
- Você abre mão de desempenho computacional?
- Você não precisa de uma solução distribuída?
- Está disposto a pagar mais caro que uma solução tradicional?

Se você respondeu **SIM** a todas as questões, estaria elegível a utilizar Blockchain como plataforma da solução.

Se as informações precisam ser públicas, utilize Blockchain Pública, senão utilize Blockchain Privada.

Origens

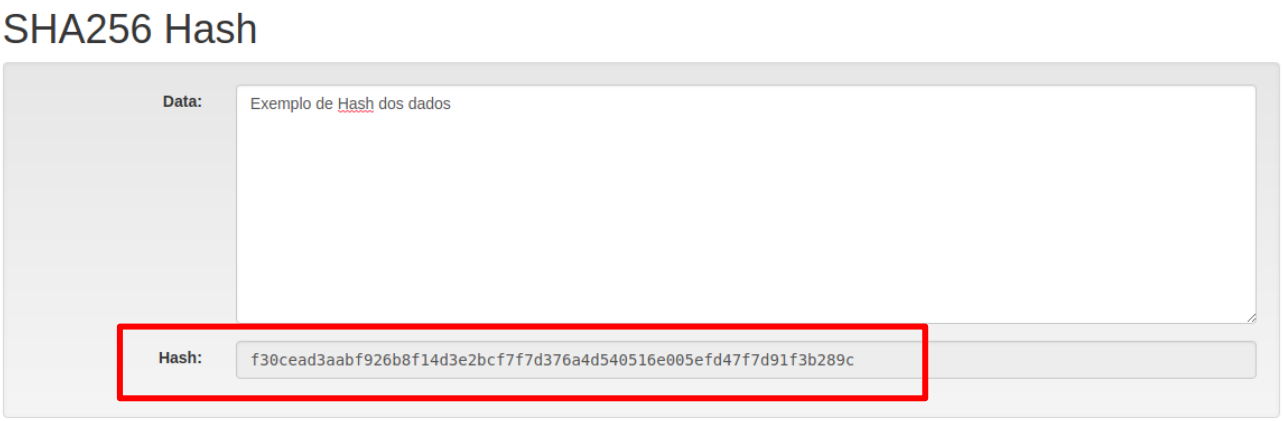
- Bitcoin: A Peer-to-Peer Electronic Cash System – Nakamoto S.

- Ideia: criar uma forma de transacionar valores eletronicamente e decentralizado que evitasse o *double spending*.
- Junção de várias técnicas já conhecidas: peer-to-peer, lista ligada, hash function, private/públic key, etc.
- Continuação do trabalhos:
  - "How to Time-Stamp a Digital Document", Haber & Stornetta, 1991.
  - "Pricing via Processing or Combatting Junk Mail", Dwork & Naor, 1993.
  - "Proofs of work and bread pudding protocols", Jakobsson & Juels, 1999.
  - "Reusable Proof-of-Work”, Finney, 2014.
  - "Hashcash - a denial of service counter-measure", Back, 2002.

Para demonstrar os conceitos, vamos usar a página: https://anders.com/blockchain/hash.html

Tecnicamente:

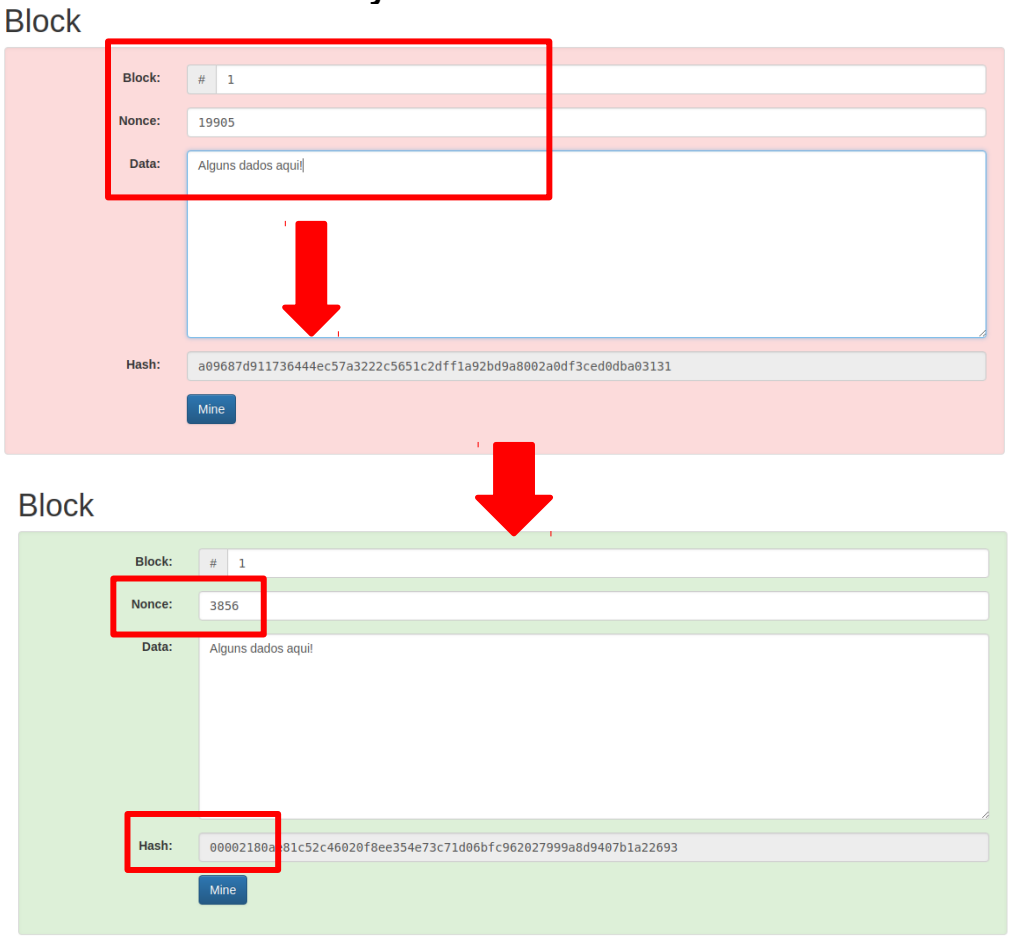
Hash Function: Exemplo SHA256



Mais detalhes: https://pt.wikipedia.org/wiki/SHA-2

"Mineração"

Calcular o **nonce** cujo o resultado do hash comece com n zeros.

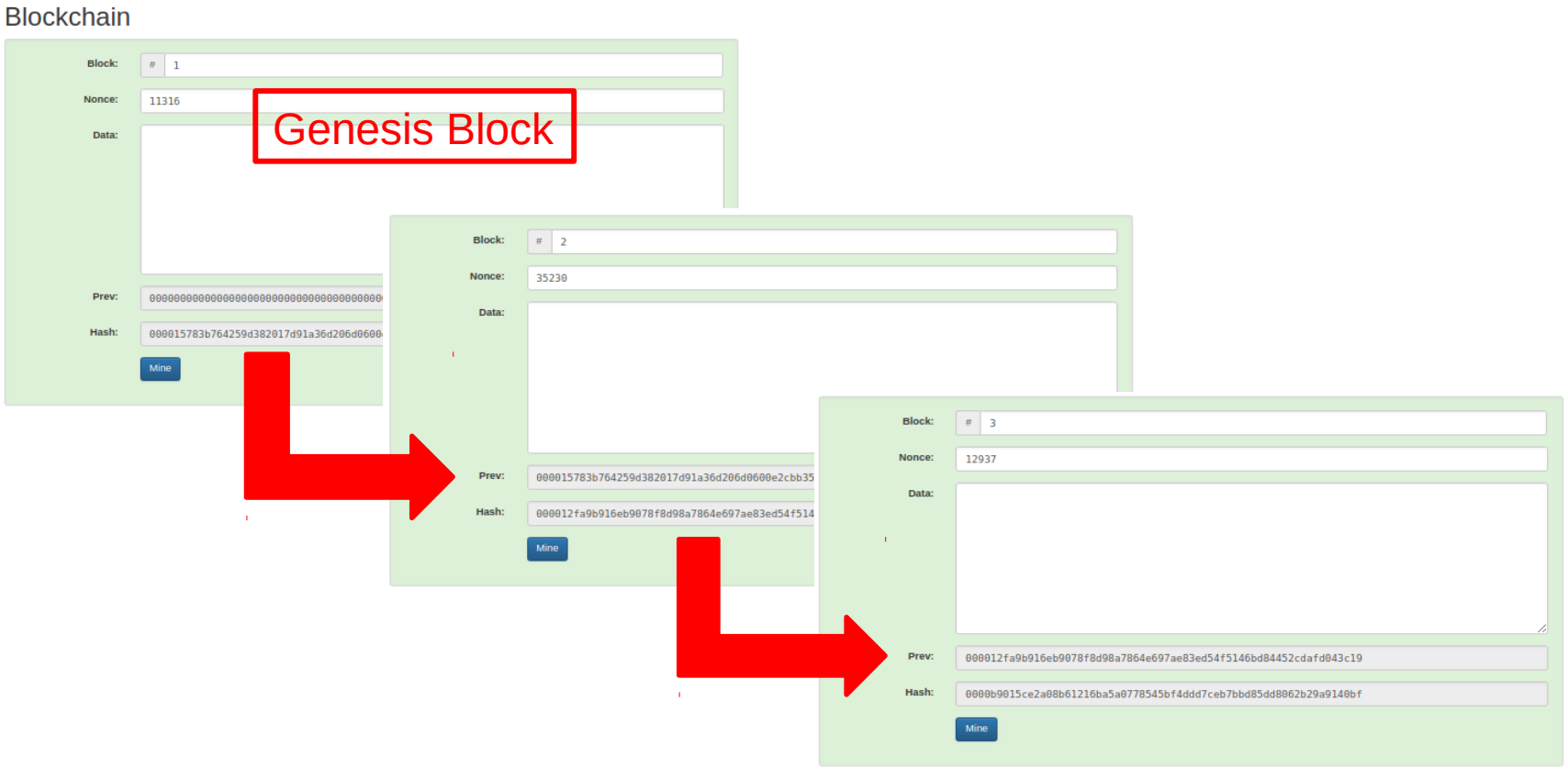


Dúvida: Existe apenas um nonce possível?

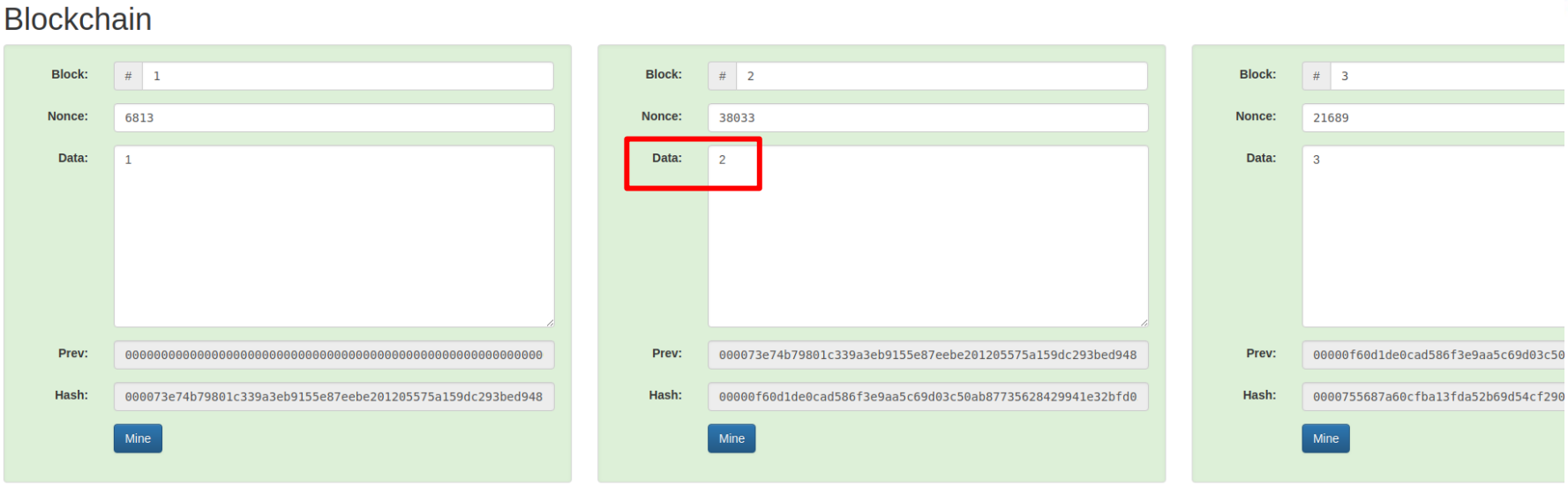
Insper

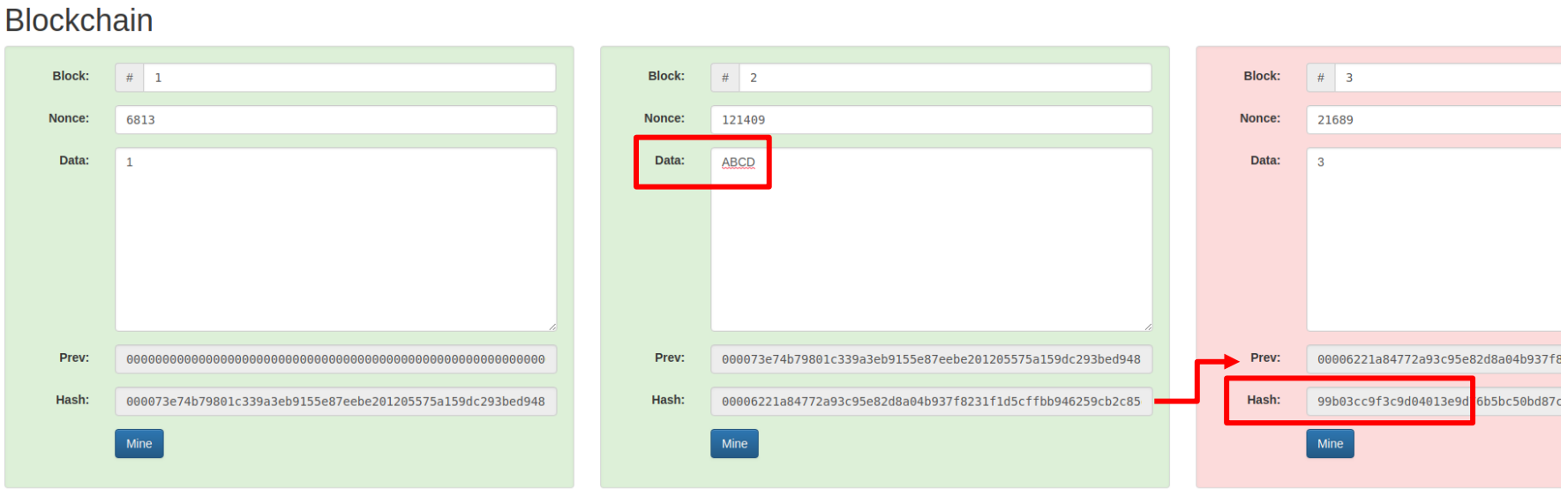
Blockchain

1. Lista ligada de blocos: O hash do bloco atual é formado pelo hash anterior + dados do bloco + nonce.



Pulo do gato: Se alterar algo em algum bloco, o seu hash seria alterado. Minerando novamente o bloco, dificilmente o hash se manteria o mesmo. Logo a lista se tornaria inconsistente.

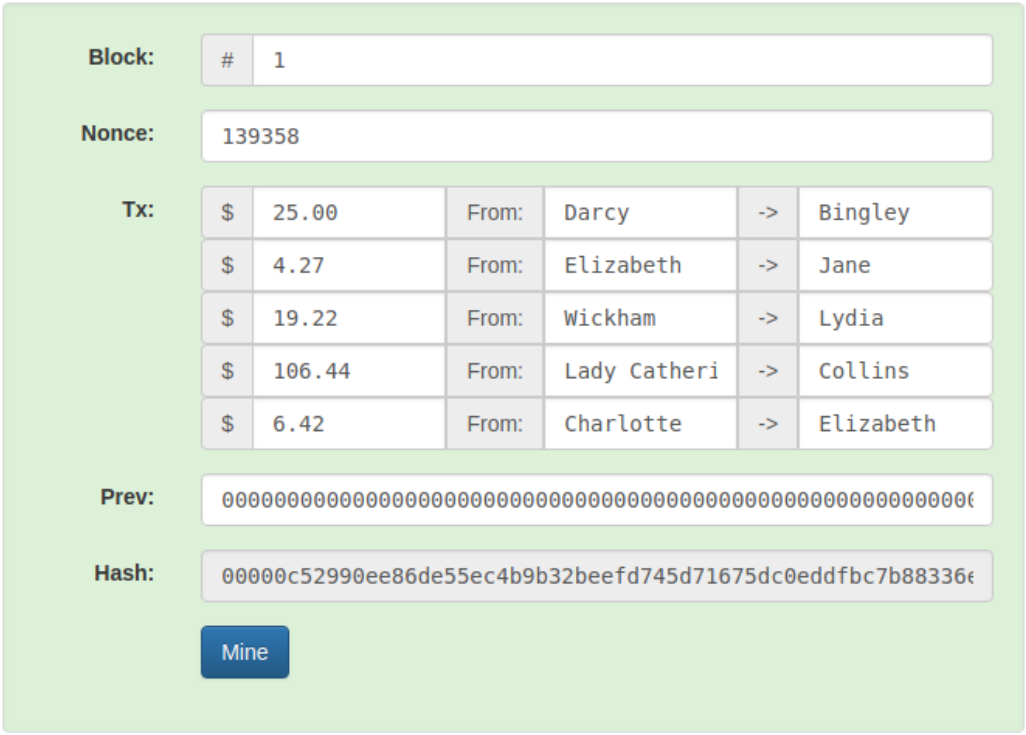




Insper

Transações

E se os dados contidos no bloco representassem transações financeiras entre duas partes:

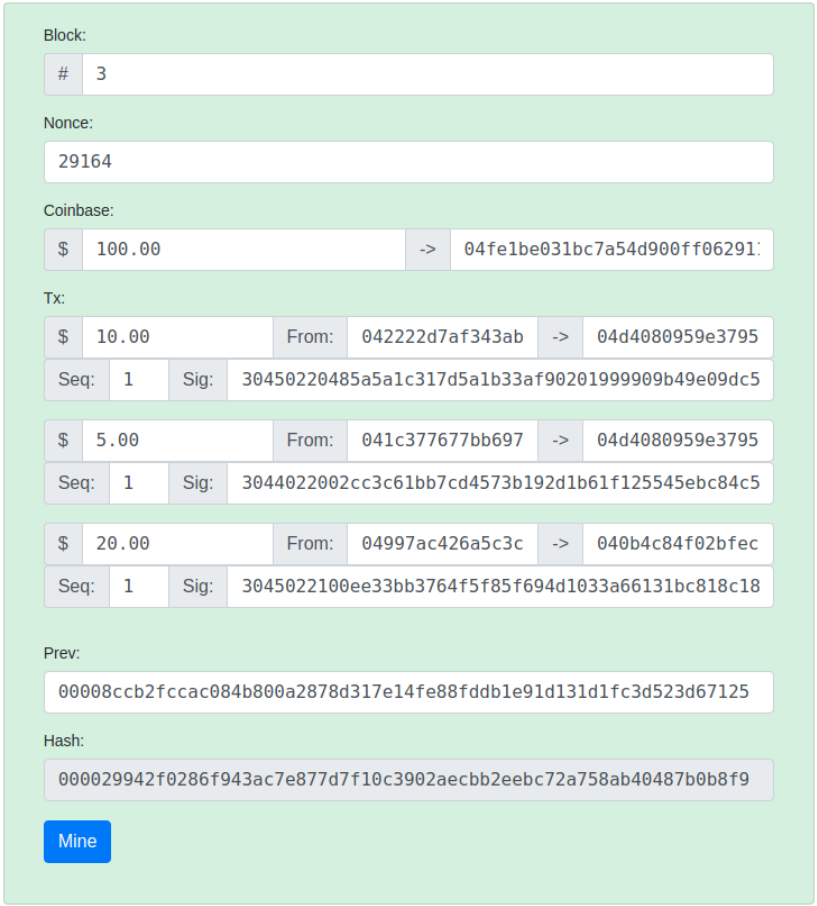


Como garantir que a transação realmente partiu da conta origem?

Transações

Assinatura: Chave pública e privada.

A origem e destino não precisa necessariamente ser identificado nominalmente:



Consenso e Votação

- Para evitar fraudes, cria-se uma rede *peer-to-peer*, onde cada nó possui uma cópia do Blockchain.
- Quando um novo nó é minerado, envia-se os dados do bloco a todos os nós da rede.
- Cada nó declara se aceita ou rejeita o bloco em questão. Caso um certo número de nós aceite o bloco, ele é incorporado ao Blockchain e começa-se a minerar um novo bloco.
- Durante a análise do bloco, os nós também avaliam a validade dos dados, e no caso de transações financeiras, se haveria saldo suficiente para efetuar cada transação.
- Caso o nó enviado seja inválido, se o minerador insistir em incorporar o bloco, ele irá divergir do resto da rede (fork).

Coinbase

- Equilíbrio do jogo: Qual o incentivo dos nós para minerar e manter uma cópia dos dados? Isso custa dinheiro.
- Ideia do Bitcoin: cada bloco minerado atribui um certo valor para a conta do minerador. Ainda, cada transação registrada paga um valor para o minerador do bloco.

- Dúvida: É possível haver um Blockchain sem uma moeda atrelada?

Forking

- O que acontece se dois mineradores acharem o bloco ao mesmo tempo?
- Como em um sistema de "votação" quem obter a maioria dos nós reconhecendo o bloco, venceria o pleito. Durante a divergência, cada nó cria um fork na lista e vai empilhando. Quando o consenso é atingido, descarta-se o ramo preterido.

- No caso extremo, pode haver cisão e haver duas redes diferentes. Em alguns casos o fork é intencional (troca de configuração, divergências permanente entre nós, etc).